



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,687	06/20/2003	Philip D. MacKenzie	15	6727
7590 01/16/2007 Ryan, Mason, & Lewis, LLP 90 Forest Avenue Locust Valley, NY 11560			EXAMINER SON, LINH L D	
			ART UNIT 2135	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE			MAIL DATE	
3 MONTHS			01/16/2007	
			DELIVERY MODE PAPER	

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Office Action Summary**

Application No.

10/600,687

Applicant(s)

MACKENZIE, PHILIP D.

Examiner

Linh LD Son

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 20 June 2003.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 June 2003 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)   | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date <u>08/03</u> | 6) <input type="checkbox"/> Other: _____  |

### **DETAILED ACTION**

1. This Office Action is responding to the filing of the application\* received on 06/20/2003.
2. Claims 1-16 are pending.

### ***Drawings***

3. The drawings filed on 06/20/2003 are acceptable subject to correction of the informalities indicated on the attached "Notice of Draftsperson's Patent Drawing Review," PTO-948. In order to avoid abandonment of this application, correction is required in reply to the Office action. The correction will not be held in abeyance.

### ***Claim Rejections - 35 USC § 102***

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2135

5. Claims 1-2, 4-6, 8-10, 12-14, and 16 rejected under 35 U.S.C. 102(e) as being anticipated by Cramer et al, US Patent No. 6697488, hereinafter "Cramer".

6. As per claim 1:

Cramer discloses "A method for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme" in (Col 6 lines 10-15), the method comprising the steps of:

obtaining the ciphertext in the first party device (Col 8 lines 25-35, encrypted plaintext); and

"generating in the first party device a plaintext corresponding to the ciphertext based on assistance from a device associated with a second party, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme" in (Col 8 line to Col 10 line 5) { Section IV teaches a verification steps to check the received ciphertext. Section V teaches steps of decrypting the received and verified ciphertext with the assistance of the sender} (Cramer and Shoup cryptographic system invention).

7. As per claims 2 and 10:

Cramer discloses "The method of claims 1 and 9, wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation" in (Col 7 lines 1-40, and Col 9 lines 25-45) {The public key is  $g_1$ ,  $g_2$ ,  $c$ ,  $d$ , and  $h$ . The exchanged information is  $z$ }.

8. As per claims 4 and 12:

Cramer discloses "The method of claim 1, wherein the generating step further comprises:

generating a share of a random secret;

generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext" in (Col 7 lines 10-27) {private key  $Z$ , and the random group};

transmitting at least the encrypted information to the second party device" in (Col 46-57); and

"computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device" in (Figure 3, Col 9 lines 25-50).

Art Unit: 2135

9. As per claims 5 and 13:

Cramer discloses "The method of claims 1 and 9, wherein the first party device and the second party device additively share components of a private key" in (Col 7 lines 10-15, and Col 9 lines 35-40).

10. As per claims 6 and 14:

Cramer discloses "The method of claims 1 and 9, wherein the generating step further comprises generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party" in (Col 8 line 38 to Col 9 line 23).

11. As per claim 8:

Cramer discloses "A method for use in a device associated with a first party for assisting in decrypting a ciphertext according to a Cramer-Shoup based encryption scheme, the method comprising the steps of:

receiving a request generated in and transmitted by a second party device for the partial assistance {*the partial assistance is the steps to verify the ciphertext before going through the decryption process in section V*} of the first party device in decrypting the ciphertext according to the Cramer-Shoup based encryption scheme; and

Art Unit: 2135

generating results in the first party device based on the partial assistance provided thereby for use in the second party device to complete decryption of the ciphertext" in (Col 8 line to Col 10 line 5) { *Section IV teaches a verification steps to check the received ciphertext. Section V teaches steps of decrypting the received and verified ciphertext with the assistance of the sender*} (*Cramer and Shoup is the inventor of this prior art.*).

12. As per claims 9 and 16:

Apparatus for use in a device associated with a first party for decrypting a ciphertext according to a Cramer-Shoup based encryption scheme" in (Col 6 lines 10-15), the apparatus

comprising:

a memory; and

at least one processor coupled to the memory " in (Col 6 lines 54-60) and

operative to:

"(i) obtain the ciphertext in the first party device" in (Col 8 lines 25-35, encrypted plaintext); and

“(ii) generate in the first party device a plaintext corresponding to the ciphertext based on assistance from a device associated with a second party, the plaintext representing a result of the decryption according to the Cramer-Shoup based encryption scheme” in (Col 8 line to Col 10 line 5) { Section IV teaches a verification steps to check the received ciphertext. Section V teaches steps of decrypting the received and verified ciphertext with the assistance of the sender} (Cramer and Shoup cryptographic system invention).

***Claim Rejections - 35 USC § 103***

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.



Art Unit: 2135

14. Claims 3, 7, 11, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cramer in view of Ronald Cramer et al, "Multiparty Computation from Threshold Homomorphic Encryption".

15. As per claims 3 and 11:

However, Cramer does not disclose "The method of claims 1 and 9, wherein the generating step further comprises an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique having a homomorphic property.

Nevertheless, Ronald Cramer does disclose the encryption technique having a homomorphic property starting on page 18.

Therefore, it would have been obvious for one having ordinary skill in the art at the time of the invention was made to incorporate as evidenced in both prior arts of the same inventor.

16. As per claims 7 and 15:

However, Cramer discloses "The method of claims 6 and 14, wherein the proofs are consistency proofs based on three-move .SIGMA.-protocols.

Nevertheless, Ronald Cramer does disclose the proofs are based on three move .SIGMA. protocols starting on page 13.

Therefore, it would have been obvious for one having ordinary skill in the art at the time of the invention was made to incorporate as evidenced in both prior arts of the same inventor.

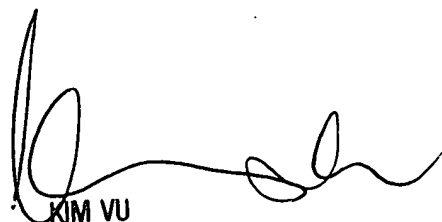
Art Unit: 2135

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son  
Examiner  
Art Unit 2135



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100